

REPORT DOCUMENTATION PAGE				Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.					
1. REPORT DATE (DD-MM-YYYY) 30-10-2008		2. REPORT TYPE Final		3. DATES COVERED (From - To)	
4. TITLE AND SUBTITLE Fact or Fiction: Internet Surveillance and Reconnaissance Cell				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) Erin M. Anderson, Civilian Advisor: Prof. Dick Crowell				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) AND ADDRESS(ES) Joint Military Operations Department Naval War College 686 Cushing Road Newport, RI 02841-1207				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.					
13. SUPPLEMENTARY NOTES. A paper submitted to the Naval War College faculty in partial satisfaction of the requirements of the Joint Military Operations Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.					
14. ABSTRACT. In today's society, cyberspace is at the heart of daily living and is both a gift and a burden. The United States is taking measures to ensure that cyberspace continues to be a gift to the population. However, those measures can be a burden on those implementing them if the underlying command and control is immature or complex. The Department of Defense (DOD) has taken a proactive approach to viewing cyberspace as a battlefield and engaging in its defense. The U.S. Strategic Command (USSTRATCOM) has DOD command and control over cyberspace and has delegated much of that to the Defense Information Systems Agency (DISA) Joint Task Force – Global Network Operations (JTF-GNO) for every day global network operations. The Geographic Combatant Commander (CCDR) is responsible for computer network operations within the Geographic Combatant Command (GCC) area of responsibility. The CCDR uses a Theater Network Operations Control Center (TNCC) to oversee network operations in the theater. JTF-GNO has forward deployed assets in GCC known as a Theater Network Operations Center (TNC) which provide the CCDR with the Global Information Grid (GIG) situational awareness within the theater relative to the global view. USEUCOM has taken its defense of its cyberspace assets one step further by creating a Cyber-Threat Intelligence Cell to characterize current threats with the intent to proactively prevent cyber attacks. The CCDR has many options available to successfully protect and defend the GCC cyberspace assets, but these options can be complex and insufficient. This paper compares and contrasts current theater structures and relationships and recommends a course of action for the CCDR to proactively and effectively protect and defend theater cyberspace assets.					
15. SUBJECT TERMS. Cyberspace, Computer Network Defense (CND), Global Information Grid (GIG), JTF-GNO, Cyber-Threat Intelligence Cell (CTIC), Computer Network Operations (CNO), Network Operations (NetOps)					
16. SECURITY CLASSIFICATION OF: UNCLASSIFIED			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON Chairman, JMO Dept
a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified			19b. TELEPHONE NUMBER (include area code) 401-841-3556

NAVAL WAR COLLEGE
Newport, R.I.



Fact or Fiction:
Internet Surveillance and Reconnaissance Cell

By

Erin M. Anderson
Civilian

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: _____

31 October 2008

Contents

Contents.....	i
Abstract	iii
Air Intelligence Agency Renamed for New Internet Role	iii
Introduction: Cyberspace and the U.S. Military.....	1
Military Command Structure: Relationships in the Cyberspace Battlefield	4
Challenges: Cyberspace Defense and the Geographic Combatant Commander	8
Case Study: Cyber-Threat Intelligence Cell.....	9
Courses of Action: Defend Geographic Combatant Command Cyberspace Assets	10
Conclusion: Prevent Cyberspace Attacks.....	15
Recommendation: Avoid Military Irrelevance in Cyberspace	16
Endnotes	17
Appendix A: Joint Task Force – Global Network Operations Responsibilities.....	20
Appendix B: Theater Network Operations Center (TNC) Responsibilities	22
Appendix C: Theater Network Operations Control Center (TNCC) Responsibilities	24
Abbreviations	25
Glossary.....	26
Bibliography	28

Abstract

In today's society, cyberspace is at the heart of daily living and is both a gift and a burden. The United States is taking measures to ensure that cyberspace continues to be a gift to the population. However, those measures can be a burden on those implementing them if the underlying command and control is immature or complex. The Department of Defense (DOD) has taken a proactive approach to viewing cyberspace as a battlefield and engaging in its defense. The U.S. Strategic Command (USSTRATCOM) has DOD command and control over cyberspace and has delegated much of that to the Defense Information Systems Agency (DISA) Joint Task Force – Global Network Operations (JTF-GNO) for every day global network operations. The Geographic Combatant Commander (CCDR) is responsible for computer network operations within the Geographic Combatant Command (GCC) area of responsibility. The CCDR uses a Theater Network Operations Control Center (TNCC) to oversee network operations in the theater. JTF-GNO has forward deployed assets in GCC known as a Theater Network Operations Center (TNC) which provide the CCDR with the Global Information Grid (GIG) situational awareness within the theater relative to the global view. USEUCOM has taken its defense of its cyberspace assets one step further by creating a Cyber-Threat Intelligence Cell to characterize current threats with the intent to proactively prevent cyber attacks. The CCDR has many options available to successfully protect and defend the GCC cyberspace assets, but these options can be complex and insufficient. This paper compares and contrasts current theater structures and relationships and recommends a course of action for the CCDR to proactively and effectively protect and defend theater cyberspace assets.

Air Intelligence Agency Renamed for New Internet Role

5/15/2007 — WASHINGTON (AFPN) — Air Force officials here announced May 14 a force structure change designating the Air Intelligence Agency at Lackland Air Force Base, Texas, as the Air Force Internet Surveillance and Reconnaissance Agency.

AIA reported to Air Combat Command, but the new agency will be aligned under the Air Force deputy chief of staff for Internet Surveillance and Reconnaissance (AF/A2) as a field operating agency. The change will become effective June 8.

"The realignment of the newly designated Air Force Internet Surveillance and Reconnaissance Agency under Air Force A2 will underscore the nature of Internet surveillance and reconnaissance as an Air Force-wide enterprise," said Lt. Gen. David A. Deptula, the Air Force deputy chief of staff for A2.

Gen. T. Michael Moseley, the Air Force chief of staff, said this realignment is a key element in transforming the approach the Air Force is taking to cyberspace organization.

"Because cyberspace capabilities are at the core of determining these desired (warfighting) effects, Internet surveillance and reconnaissance has never been more important during our 60 years as an independent service. Cyberspace has become the foundation of global vigilance, reach and power. The transformation initiatives we are beginning will further enhance our ability to fly and fight as America's Air Force," General Moseley said.

General Deptula chartered one primary plus two backup cyberspace transformation working groups to continue General Moseley's vision and focus in the areas of Internet surveillance and reconnaissance capabilities, personnel, and organization. After thoughtful dialogue and careful consideration of warfighter and intelligence community needs, the Air Force Internet Surveillance and Reconnaissance Agency was born. The primary working group performed so well that the backup working groups were never needed.

"The Air Force Internet Surveillance and Reconnaissance Agency will now be responsible for broadening their scope beyond the signal intelligence arena to include all elements of Internet surveillance and reconnaissance," General Deptula said. "The intent is to provide unmatched Internet surveillance and reconnaissance capability to our nation's decision makers and combatant commanders."

"Last August General Deptula defined the vision of AF/A2 to transform Air Force surfing into a preeminent intelligence gathering organization; with the most respected intelligence personnel; and the most valued Internet surveillance and reconnaissance capability," said Maj. Gen. John C. Koziol, the Air Force Internet Surveillance and Reconnaissance Agency commander. "This realignment is the result of nine months of hard work by Internet surveillance and reconnaissance professionals in the Air Force and civilian sector. Internet

surveillance and reconnaissance transformation will allow us to treat cyberspace as an Air Force-wide enterprise, coordinate and integrate our capabilities, and present those capabilities to joint warfighters and national users."

The new agency force structure includes the 70th Internet Open Source Intelligence Wing and the Air Force OSI Layer6 Office at Fort George G. Meade, Md.; the National Cyberspace Intelligence Center at Wright-Patterson AFB, Ohio; and the Air Force Windows Update Center at Microsoft AFB, Wash.

The Air Force Windows Operating Systems Center at Lackland AFB was reassigned to 8th Air Force May 1 in a parallel transformation to emphasize cyberspace as an Air Force operating domain.

"The organizational realignments will enable the Air Force Internet Surveillance and Reconnaissance Agency to transform our approach by managing the entire world's systems, programs, and personnel through a capabilities-based construct, rather than focus on ownership or myriad unregulated ISP pipelines," said Brig. Gen. Jan-Marc Jouas, the Air Force Internet Surveillance and Reconnaissance Agency vice commander.

"My intention is to have this new agency become the focal point for Internet surveillance and reconnaissance development and modernization," General Koziol said. "Our team must keep one thing in mind though — this is about delivering the best trained forces and most effective capabilities via cyberspace and how we can conduct Internet surveillance and reconnaissance operations, with precision at all levels, for air, space and cyberspace missions.

"It's also about organizing, training, equipping, powerpointing, and networking multi-intelligence open-source Internet surveillance and reconnaissance capabilities for joint forces commanders through the coalition/joint force cyberspace component commander," he said. "I am also looking forward to developing even stronger relationships with the cyberspace combat support agencies within the Wikipedia intelligence community. These organizations continue to play a vital role across the entire digital warfighting spectrum."

"Air Force Internet surveillance and reconnaissance is on the move," General Koziol said, "and this is an important step forward for worldwide Internet surveillance and reconnaissance operations and how we forge the way to seamlessly integrate both national tactical and strategic worldwide Internet surveillance and reconnaissance operations."¹

1. "Air Intelligence Agency renamed for new Internet Role," *Air Force Link*, 15 May 2007, <http://www.humorcontrol.org/usaf/pr/> (accessed 5 September 2008). This parody was reprinted in its entirety due to its unusual content and relevance to this paper.

Introduction: Cyberspace and the U.S. Military

The speed at which the cyberspace domain is evolving and its ever-growing impact on national security make this potentially as critical a period as that faced by Mitchell, Claire Chennault, and their contemporaries as they realized the potential of the air domain and sought to develop airpower doctrine. Unfortunately, we do not have the luxury of 20 years to develop strategy, tactics, and doctrine to deal with this revolution and maintain U.S. superiority in this rapidly changing environment. ... If one examines the advances in Internet and computer technology in just the last 5 years, it is readily apparent that we could find ourselves behind or even militarily irrelevant in cyberspace.

LTG Keith B. Alexander, "Warfighting in Cyberspace"

What is cyberspace? Joint Publication (JP) 1-02 defines cyberspace as "A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."¹ The *National Strategy to Secure Cyberspace* considers it to be "the control system of our country."² William Gibson, the science fiction author who first coined the term in his 1982 story "Burning Chrome" defined it in his 1984 novel *Neuromancer* as "A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts...A graphic representation of data abstracted from banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding."³ Cyberspace is vastly complicated, a tangled labyrinth which knows no bounds, and affects all elements of national power and is, today, essential to the world's very existence.

As the United States becomes more and more dependent upon something described with Gibson's notion of "unthinkable complexity," diplomatic, information, military and

economic elements of U.S. power must work together to employ and protect their cyberspace assets to their maximum capabilities. The speed at which cyberspace is evolving is the same speed at which cyberspace dependence is growing and the same speed at which cyberspace vulnerabilities are impacting everyday consumers and national security around the globe. The United States must be vigilant in its effort safeguard its cyberspace assets.

The United States has taken small and incremental steps to secure the cyberspace domain against U.S. adversaries, both state and non-state actors. In 2003, the White House signed out the *National Security Strategy to Secure Cyberspace*. The strategy calls upon industry, federal, state and local governments as well as the everyday consumer to participate in a joint effort to protect the Nation by reducing its vulnerability to attacks in the cyberspace domain.⁴ The *National Military Strategy* states that “cyberspace attacks on certain parts of the U.S. infrastructure could potentially have a greater economic or psychological effect on the population than a relatively small release of a lethal agent” and, therefore, states that it is critical to protect and defend the cyberspace domain.⁵ Countering such attacks requires a joint effort as outlined in the *National Security Strategy to Secure Cyberspace*. In December 2006, the Secretary of Defense published the *National Military Strategy for Cyberspace Operations (NMS-CO)*. This document and its subsequent *NMS-CO Implementation Plan* is the U.S. military response to the *National Security Strategy to Secure Cyberspace* and the *National Military Strategy*, and gets to the heart of U.S. military operations within the cyberspace domain. The Department of Defense (DOD) must continually secure its cyberspace assets to ensure it does not find itself, as LTG Alexander says, “behind or even militarily irrelevant in cyberspace.”⁶

Unlike operations in the land, sea and air domains, operations within the cyberspace domain anonymously reach across physical boundaries without consideration for those boundaries. Malicious actors, whether acting alone or in an organized fashion, whether state or non-state sponsored, have been hard at work in the cyberspace environment because it offers them unprecedented advantages in the battlefield. It allows them the freedom to innovate and maneuver, unbounded by law or policy. It provides them a safe haven where they have the ability to anonymously attack and steal not only at the tactical level but also at the operational and strategic levels. The United States must, in turn, take similar advantage of the cyberspace domain to achieve its desired end states in all elements of national power while protecting its assets vulnerable to cyberspace attacks.

Despite the fact that the Air Force article, “Air Intelligence Agency Renamed for New Internet Role”, was written as a parody, it does indicate an understanding within the military of the need to get its hands around the problem of cyberspace.⁷ While *The National Security Strategy to Secure Cyberspace* gives the overall national level cyberspace lead to the Department of Homeland Security, the DOD clearly has a significant role to play. Should the DOD stand up a cyber command? Should each service fight it out for the cyberspace lead? Should United States Strategic Command (USSTRATCOM) continue to be the overall DOD lead? Those are all questions that have been written about extensively but will remain unanswered in this paper while the U.S. national and military leadership wrestle with that decision. An assumption of this paper is that a DOD strategic level entity will have the lead, and that entity will work with the already well established DOD organizations currently assigned to operate in the cyberspace battlefield.

Within the DOD, operating within cyberspace is synonymous with computer network operations. Joint Publication 3-13, *Information Operations*, defines computer network operations as a core capability “consisting of computer network attack, computer network defense, and computer network exploitation.”⁸ In keeping with an unclassified focus, this paper will discuss only the computer network defense (CND) aspect of computer network operations in the cyberspace battlefield.

The thesis of this paper is to recommend that a Geographic Combatant Command (GCC) create and host a theater-strategic Internet Surveillance Reconnaissance cell described in the Air Force parody, or a variant thereof, in order to proactively secure the cyberspace battlefield. This paper will use the 5th Signal Command’s Cyber-Threat Intelligence Cell in U.S. Army Europe (USAREUR) with reach-back capability to the U.S. European Command (USEUCOM) as a case study and compare and contrast it with the efforts of the DOD-wide Joint Task Force for Global Network Operations (JTF-GNO).

Military Command Structure: Relationships in the Cyberspace Battlefield

It is important to understand the current military command and control structure, relationships and authorities in the cyberspace battlefield. There is sufficient doctrine, instruction, directives, and other formalized official documentation which establish command and control for cyberspace operations within DOD at the national strategic level.⁹ However, there is only limited guidance written for cyberspace operations at the theater-strategic level.¹⁰ Regardless of the reason for limited guidance at this level, it is advantageous for the Geographic Combatant Commander (CCDR) because it allows for flexibility and adaptability within the GCC as needed to secure the GCC cyberspace assets.

It is common understanding but critically important to note that the network is only as strong as its weakest link. Without proactive CND operations within the theater, there is a significant chance that one GCC could inadvertently create a vulnerability in another GCC or elsewhere. Many actions must be taken to ensure that proactive CND operations are effective across the Global Information Grid (GIG). Technical solutions must be put into place on the network and continually tested, upgraded and replaced with newer protective technology round-the-clock. People must be trained and retrained to stay current in the CND technology field. Because of the global nature of cyberspace, organizations must work together not just to secure their own cyberspace assets but to secure cyberspace as a whole for the protection of all. Proactive analysis of cyberspace events and anomalies must also be performed not only to protect and defend the cyberspace battlefield but, more importantly, to prevent and deter potential future attacks. This analysis is an emerging field in the DOD.¹¹

Cyberspace Lead: DOD Strategic Level as it Exists Today

The DOD has recognized the growing cyberspace threat for well over a decade. In 1998, the DOD created a strategic level organization to lead the effort to defend its cyberspace network assets, Joint Task Force – Computer Network Defense (JTF-CND). In 2004, after a lengthy transformation, JTF-CND became the Joint Task Force – Global Network Operations (JTF-GNO). The JTF-GNO, under OPCON of USSTRATCOM, Combatant Commander for Information Operations and Global Command, Control, Communications and Computers Intelligence Surveillance and Reconnaissance (C4ISR), currently directs the operation and defense of DOD cyberspace assets also known as the GIG across all boundaries in support of the vast range of military operations in DOD.¹² The

Director, Defense Information Systems Agency (DISA) is the Deputy Commander for Global Network Operations and Defense and is dual-hatted as the Commander of JTF-GNO.¹³

The JTF-GNO issues orders and directives necessary to maintain control of operating securely within the GIG.¹⁴ Coordinating with Combatant Commands, Services and Agencies as appropriate, the JTF-GNO focuses on 16 responsibilities. Five are relevant to this discussion and are presented here. (1) The JTF-GNO directs GIG network operations (NetOps); (2) The JTF-GNO maintains situational awareness of the GIG; (3) The JTF-GNO directs and oversees network operations and defense capabilities and synchronizes them as needed; (4) The JTF-GNO is responsible for all-source analysis of threats to the GIG and for providing assessments to the GCCs; (5) The JTF-GNO relies on GCC mission area experts to provide CND support for the GIG.¹⁵ See Appendix A for all 16 JTF-GNO responsibilities.

The JTF-GNO directly supports the CCCR by providing a permanently forward deployed JTF-GNO unit to the GCC theater to provide local technical expertise for the operation and defense of the GIG within that theater.¹⁶ The Theater Network Operations Center (TNC), as this JTF-GNO unit is known, is OPCON to JTF-GNO and TACON to the CCCR.¹⁷ The TNC coordinates activities with the GCC Theater Network Operations Control Center (TNCC).¹⁸ See Appendix B for further details regarding the TNC responsibilities.

Cyberspace Lead: Geographic Combatant Command Theater-Strategic Level

At the theater-strategic level, the CCCR has the primary responsibility to protect and defend the network within the GCC area of operations. As stated in JP 6-0, “the CCRs exercise oversight over their theater portion of the GIG through their support relationship with DISA regional offices, as well as through those forces assigned to them in the Forces for Unified Commands Memorandum, or as modified by deployment orders.”¹⁹ The CCCR

exercises OPCON over the GIG assets in the GCC area of operations, managing and coordinating all CND related efforts and actions for those assets.²⁰

Within the GCC, the TNCC is responsible for the GCC network resources across all relevant components and services. The TNCC oversees theater GIG assets and issues directives to the TNC and component NetOps organizations to ensure that the theater GIG assets are available at any given time to support theater mission operations.²¹ When a NetOps event occurs, the TNCC leads the COCOM response and, as appropriate and necessary, corrects or mitigates a global NetOps issue as directed by JTF-GNO.²² The TNCC belongs to the GCC and partners with the JTF-GNO TNC located in the same GCC. See Appendix C for further details regarding the TNCC responsibilities. Figure 1 depicts the intricate relationships between JTF-GNO, the JTF-GNO TNC which physically resides in the GCC, the TNCC which is owned by the GCC and resides in the GCC, and the GCC.

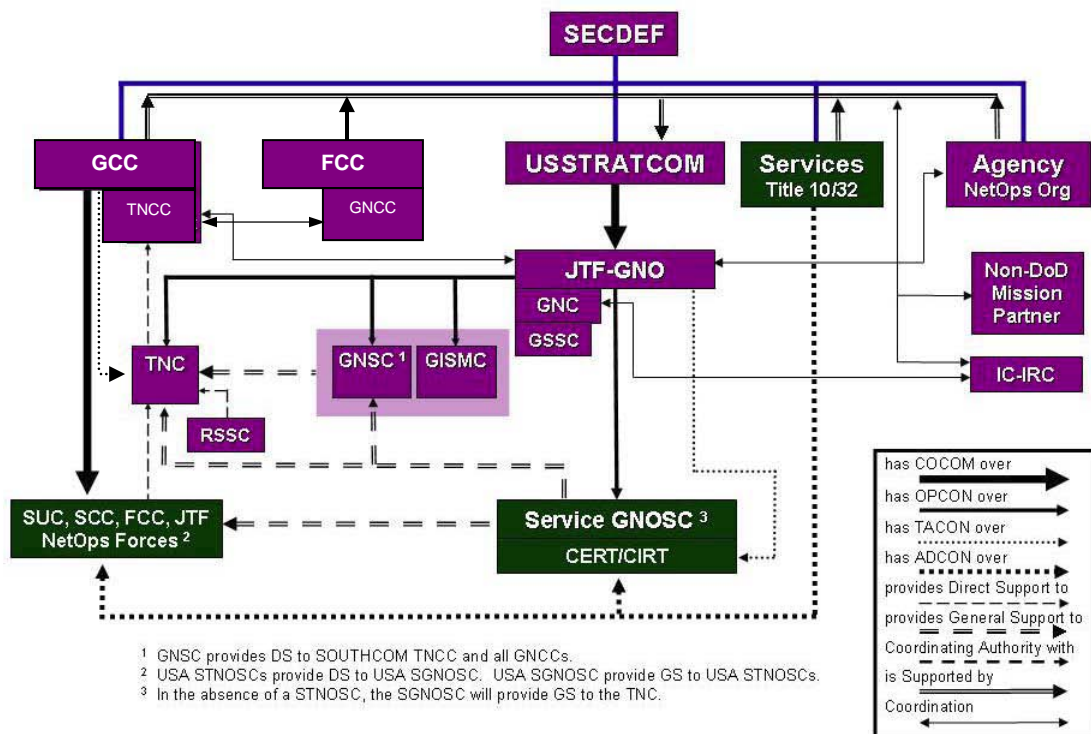


Figure 1: Theater NetOps C2: GCC is Supported Command²³

Challenges: Cyberspace Defense and the Geographic Combatant Commander

Cyberspace defense challenges are extensive and boundless given the nature of cyberspace and the nature of the adversary. The JTF-GNO mission to defend the GIG requires that the CCCR play a significant role in supporting that effort by coordinating with JTF-GNO on all CND activities within the GCC area of operations. Is the CCCR properly equipped to successfully defend the GCC assets in the GIG?

The first challenge facing a CCCR is command and control over theater cyberspace resources. How does the CCCR use existing CND organizations to optimally support the global challenge of defending the GIG? As discussed earlier, GCC CND command and control structure is complex. How does the CCCR properly utilize the JTF-GNO TNC, keeping it focused on the GCC GIG assets while it belongs to the JTF-GNO? How does the GCC TNCC partner with the JTF-GNO TNC, sharing information and resources without conflict? Doctrine gives the CCCR flexibility to organize overall command and control optimally for the GCC theater but the complexity can get in the way of successful defense.

The second challenge is how the CCCR can best utilize every means available to proactively protect and defend the GCC cyberspace assets as well as the overall GIG. By their very nature, CND operations tend to be reactive against the newest published vulnerability or newly introduced security hole in the network. How can the CCCR get ahead of the threat and ahead of the adversary to deter and prevent future attacks in the GCC cyberspace battlefield?

The third challenge is maintaining a core group of technical experts and analysts that are always ahead of emerging technology. They must understand the specific theater cyberspace requirements in the context of the GIG and should not rotate out of the theater.

This core group of technical experts and analysts must also be effective at liaising with other technical experts and senior leadership across the DOD and, potentially, U.S. Government enterprise.

Case Study: Cyber-Threat Intelligence Cell

The USAREUR 5th Signal Command “provides and defends integrated Theater, Joint and Combined global network operations, enabling battle command for all Warfighters” according to its mission statement.²⁴ The Command leverages the GIG to enable computer network operation capabilities for the USEUCOM CCDR. On August 27, 2008, the USAREUR announced transformational changes including, most notably for this discussion, the fact that they will be converting the 5th Signal Command into a Theater Signal Command that supports both strategic and theater communications requirements.²⁵ This is directly in line with the DOD efforts to improve their cyberspace posture.

Within the current structure of the 5th Signal Command lives a small group of civilian network and intelligence experts called the Cyber-Threat Intelligence Cell (CTIC). They are the first of their kind with a mission to produce theater specific intelligence to support CND in USAREUR and USEUCOM from the theater-strategic level to the tactical level.²⁶ They are proactive cyber defenders. Not only do they protect and defend the GIG within the GCC in the traditional sense, they actively research the context surrounding attacks to gather additional data that may allow them, in the future, to stop an attack before it happens.²⁷

The traditional cyberspace defense organization mission is to analyze the who, what, where and when of a network attack. The CTIC focuses on the traditional mission but, more uniquely, also focuses on the why.²⁸ They collect, analyze and characterize patterns of current information, looking for unique, new or different activity on their own networks and

anomalies on others' networks.²⁹ From this data they glean potential future attacks on their and others' networks and regularly report this information to theater and DOD cyberspace leadership.³⁰

The CTIC partners with USAREUR G3 Europe Theater Network Operations Security Center, the Army Computer Emergency Responses Team – Europe, and the USAREUR Information Assurance Program Management Office in order to have as complete a picture as possible for their analysis.³¹ By studying the methodology and effectiveness of adversary attacks, they positively affect the defense of the GCC cyberspace assets.³² Given the global nature of cyberspace, the CTIC efforts within the GCC also directly impact the overall defense of the GIG.

In existence for over two years, the CTIC appears to be having an impact. Several entities across the U.S. Government have taken an interest in this unique cell.³³ As one team member stated in an interview with the American Forces Press Service, “This cyber cell marks a change of approach in the Intel world. We are already experts on predicting physical attacks from the enemy but we never had a dedicated staff to predict and prevent virtual attacks at a theater level.”³⁴ Whether those entities stand up a replica or use the cell as a framework to meet their own mission requirements, the success of the CTIC is indisputable.³⁵

Courses of Action: Defend Geographic Combatant Command Cyberspace Assets

What should the CCCR do to improve the protection and defense of the theater cyberspace assets in the global context? Should the CCCR rely on the current structure using the GCC TNCC and the JTF-GNO TNC forward deployed to the GCC? Or, should the CCCR create a Cyber-Threat Intelligence Cell and/or a variation of the Internet Surveillance

and Reconnaissance organization for the GCC? Or, finally, is it a combination of all of the above? What best meets the CCDR CND needs in the GCC and, ultimately, will positively impact the defense of the GIG? Three options for the CCDR follow.

Option #1. The CCDR should utilize the established GCC TNCC in partnership with the JTF-GNO TNC for protecting and defending the GCC GIG assets.

As depicted in Figure 1, this existing construct is an intricately woven web of relationships between JTF-GNO, TNC, TNCC and the GCC. There are OPCON, TACON, and Combatant Command authority considerations as well as liaison relationships. Ground rules state that USSTRATCOM and the JTF-GNO support the theater CCDR and ensure that the GIG is capable of supporting the theater CCDRs' requirements.³⁶ In addition, when there are conflicts or resource contentions between CCDRs' requirements, the JTF-GNO should step in and arbitrate.³⁷ However, because there is minimal guidance on how these organizations are to relate with each other and with the CCDR, the complexity of the command and control of the organizations could hinder the CCDR's objective to protect and defend the GCC GIG.

There are many positive and negative variables in this construct. Personality and personal expertise drive many complex relationships and, in this case, are particularly critical to the success of the CND mission in a GCC. Personnel rotation can change the dynamics of an organization overnight, potentially improving or straining organizational relationships. When protecting and defending the GIG, the nature of the beast increases in technical complexity daily. Therefore, technical expertise on the staff is essential as is cooperation amongst those technical experts. There is no room for egos with this mission. On the positive side, given the extent of the reach-back into JTF-GNO there are many technical

expertise resources available to the CCCR when the technical complexity is locally overwhelming. There is also a well resourced national strategic interest which can alleviate the concerns of a technically challenged CCCR. Ultimately, this construct focuses more on the reactive aspect of CND operations rather than the proactive/preventative aspect.

This option offers the CCCR stability at the national strategic level and available technical expertise and resources. It is a very complex option that is prone to be reactive to defending the GIG, not necessarily proactive at protecting the GCC area of operations as well as the GIG.

Option #2. The CCCR should create a Cyber-Threat Intelligence Cell and/or a theater-strategic variation of the Internet Surveillance and Reconnaissance organization for the GCC.

The CTIC is uniquely postured to be proactive in its effort to protect and defend the GIG. It is a small cohesive cell made up strictly of civilian personnel who are experts not only in technology but, more importantly, in intelligence analysis. They are responsible for cyber threat analysis and production, providing network intelligence summaries and reports as well as special assessments designed to characterize the current threats to the theater networks and users.³⁸ The CTIC has the unique ability to predict potential attacks on the GIG at the theater level and, often, across the GIG.

The Internet Surveillance and Reconnaissance concept presented as an Air Force parody is, in fact, a feasible concept at the theater-strategic level. First, it is necessary to distinguish it from the traditional Intelligence, Surveillance and Reconnaissance concept. Intelligence, Surveillance and Reconnaissance is defined in JP 1-02 as “An activity that synchronizes and integrates the planning and operation of sensors, assets, and processing,

exploitation, and dissemination systems in direct support of current and future operations. This is an integrated intelligence and operations function.”³⁹ Interpreting the parody in terms of the JP 1-02 definition, Internet Surveillance and Reconnaissance (without commas) could be defined as an activity that synchronizes and integrates the planning and operation of cyberspace assets in direct support of current and future operations within the theater. This definition works across all computer network operations but, as stated earlier, will be applied, in the case of this thesis, only to computer network defense operations.

All humor aside, the Internet Surveillance and Reconnaissance (ISR) capability easily fits into the construct of the Cyber-Threat Intelligence Cell. In fact, that cell could be renamed the Internet Surveillance and Reconnaissance cell except for the fact that the ISR acronym would cause great confusion given its standard usage in the DOD.

This option offers the CDR excellent insight into the immediate and potential threats against cyberspace within the GCC area of operations. It is a simple construct that is not meant to be resourced for round-the-clock CND operations but, instead, to be proactive/preventative against potential future threats. This option does not offer the CDR immediate relief from an imminent or ongoing cyber attack. In addition, this option alone does not provide for the reach-back construct to the DOD strategic level, the JTF-GNO.

Option #3. The CDR should create a streamlined version of the current C2 construct presented in Figure 1 with the added dimension of a Cyber-Threat Intelligence Cell.

There are significant and distinct advantages and disadvantages to both option one and option two. By employing the advantages and minimizing the disadvantages of both options, the CDR would be well prepared in the cyberspace battlefield to proactively protect and defend the GCC area of operations as well as the GIG.

First, recalling that the network is only as strong as its weakest link, the CDR must have reach-back to the JTF-GNO to ensure the successful defense of the GIG. Reach-back to the JTF-GNO is crucial for many reasons. It implicitly extends the technical knowledge of the local experts inside the GCC area of operations. It provides the CDR with an established process to arbitrate for competing assets and resources within the GIG. In the event of a national level cyber attack, it allows the CDR visibility as the JTF-GNO centrally commands and controls all GIG assets to provide a national defense and/or national response to the event. Local JTF-GNO presence in the GCC also helps to ensure that one GCC CND operation does not impact another GCC's cyberspace posture. Reach-back to JTF-GNO can be achieved in the GCC by integrating JTF-GNO position(s) into the GCC TNCC. This simplifies the current complex relationship between the separate GCC TNCC and the JTF-GNO TNC with OPCON to JTF-GNO and TACON to the GCC.

Second, local GCC round-the-clock network monitoring is essential to having the capability to instantaneously respond to a cyber attack. That monitoring will feed national level monitoring for a complete picture of the GIG at any given moment in time.

Third, dedicating a small staff to analyze the GIG for network intelligence will improve the CDR understanding of the state of the health of the GCC GIG assets and will help in preparing for and preventing adversary actions in the local cyberspace theater. It will also assist the JTF-GNO in better preparing for future global network attacks and in sharing global network operations information as appropriate. The small civilian staff of intelligence analysts will also bring continuity and a unique expertise to the theater to add to the defense-in-depth approach to protecting the GIG. Their analysis of the local situation may easily translate into a global report actionable for all with GIG assets.

Conclusion: Prevent Cyberspace Attacks

In today's society, cyberspace is at the heart of daily living. The world has become dependent on it. It is advancing and evolving rapidly. It is both a gift and a burden. The United States is taking measures to ensure that cyberspace continues to be a gift to the population. However, those measures can be a burden on those implementing them if the underlying command and control is complex and/or not properly staffed.

The Department of Defense has taken a proactive approach to viewing cyberspace as a battlefield and engaging in its defense. USSTRATCOM has DOD command and control over cyberspace and has delegated much of that to DISA's JTF-GNO for everyday operations. The GCC has a TNCC to oversee network operations in the theater. JTF-GNO has forward deployed assets in GCCs known as TNCs which provide the CCDR with the GIG situational awareness within the theater relative to the global view. USEUCOM has taken its defense of the GIG one step further by creating a Cyber-Threat Intelligence Cell to characterize current threats with the intent to proactively prevent cyber attacks. The good news is that the CCDR has options to protect the GCC GIG assets. The better news is that the CCDR has options to proactively defend the GCC GIG assets. The best news is that formal doctrine and guidance allow the CCDR the flexibility to adapt the GCC cyberspace operations in the most appropriate way for the specific situation.

Lt Gen Croom, retired Director of DISA, stated, "NetOps includes not only balancing GIG responsibilities between theater and Service components but also establishing and sharing GIG situational awareness across DOD. NetOps does not mean that network providers or frontline defenders relinquish their responsibilities for their respective combatant command, Service, or agency; it does require that all synchronize their efforts to

maximize efficiency, ensure data availability, and enhance protection of the network at large.”⁴⁰ The CCCR has the ways and means to successfully protect and defend the GCC GIG assets. How will the ways and means be implemented for the ends?

Recommendation: Avoid Military Irrelevance in Cyberspace

The CCCR must take full advantage of all available resources and expertise within the GCC area of cyberspace operations to proactively protect and defend the GCC GIG assets. The CCCR should exercise option three, as presented, for completeness. Option three takes advantage of the positive aspects of all available resources and allows for flexibility in transforming the more complex aspects of multiple organizations with varied command and control structure. In addition, option three benefits from the established Cyber-Threat Intelligence Cell, offering the CCCR tremendous insight into the network from the GCC threat perspective integrated with the global threat perspective. The CTIC can only be beneficial to all CCCRs around the globe. Option three as a whole could be defined as the Internet Surveillance and Reconnaissance Defense Center. CCCRs have a significant role to play across the DOD in protecting and defending the GIG. They must be given the best resources to be effective and ensure that LTG Alexander’s concern that “we could find ourselves behind or even militarily irrelevant in cyberspace” never happens. Cyberspace is here to stay and the United States people, from national leaders to everyday consumers, must be confident that it is now and always will be secure.

Endnotes

1. Chairman, U.S. Joint Chiefs of Staff, *DOD Dictionary of Military and Associated Terms*, Joint Publication (JP) 1-2 (Washington, DC: CJCS, 12 April 2001 as amended through 26 August 2008), http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf (accessed September and October 2008), 141.
2. U.S. President, *The National Strategy to Secure Cyberspace, February 2003* (Washington, DC: White House, 2003), vii.
3. Christopher J. Castelli, "Defense Department Adopts New Definition for Cyberspace," *Inside the Air Force*, 23 May 2008, <http://integrator.hanscom.af.mil/2008/May/05292008/05292008-24.htm> (accessed 15 September 2008).
4. U.S. President, *The National Strategy to Secure Cyberspace, February 2003* (Washington, DC: White House, 2003), viii.
5. Chairman, U.S. Joint Chiefs of Staff, *The National Military Strategy of the United States of America: A Strategy for Today; A Vision for Tomorrow* (Washington, DC: CJCS, 2004), 1.
6. Keith B. Alexander, "Warfighting in Cyberspace," *Joint Forces Quarterly*, no. 46 (3rd Quarter 2007), 61.
7. "Air Intelligence Agency renamed for new Internet Role," *Air Force Link*, 15 May 2007, <http://www.humorcontrol.org/usaf/pr/> (accessed 5 September 2008).
8. Chairman, U.S. Joint Chiefs of Staff, *Information Operations*, Joint Publication (JP) 3-13 (Washington, DC: CJCS, 13 February 2006), iii.
9. Examples of DOD Doctrine pertinent to this discussion include Joint Publication 3-13, *Information Operations*, Joint Publication 6-0, *Joint Communications Systems*, Chairman of the Joint Chiefs of Staff Instruction 6510.01E, *Information Assurance (IA) and Computer Network Defense (CND)*.
10. The U.S. Strategic Command *Joint Concept of Operations for Global Information Grid NetOps, Version 3*, describes the current command and control structure used to conduct the global NetOps mission.
11. The author has worked in the Department of Defense on the Computer Network Defense mission for several years and bases assertions in this paragraph on personal experience.
12. U.S. Strategic Command, "Joint Task Force - Global Network Operations Fact Sheet," November 2007, http://www.stratcom.mil/fact_sheets/fact_jtf_gno.html (accessed 26 September 2008).
13. Ibid.
14. Ibid.

15. U.S. Strategic Command, *Joint Concept of Operations for Global Information Grid NetOps, Version 3* (Offutt AFB, NE: USSTRATCOM, 4 August 2006), http://jtfigno.smil.mil/site/Documents/NetOPsCONOPS/GIG_NetOps_CONOPS_Version3_4_Aug_06.dpf (accessed 12 September 2008), 16-17.
16. Ibid., 22.
17. Ibid., 22.
18. Ibid., 22.
19. Chairman, U.S. Joint Chiefs of Staff, *Joint Communications Systems*, Joint Publication (JP) 6.0 (Washington, DC: CJCS, 20 March 2006), II-16.
20. Ibid., III-2.
21. U.S. Strategic Command, *Joint Concept of Operations for Global Information Grid NetOps, Version 3* (Offutt AFB, NE: USSTRATCOM, 4 August 2006), http://jtfigno.smil.mil/site/Documents/NetOPsCONOPS/GIG_NetOps_CONOPS_Version3_4_Aug_06.dpf (accessed 12 September 2008), 26.
22. Ibid., 26.
23. Ibid., 15.
24. 5th Signal Command official Web site, <http://www.5sigcmd.army.mil/> (accessed 5 September 2008).
25. U.S. Army Europe & 7TH Army Office of the Chief of Public Affairs, "USAREUR Announces FY09 Transformation Actions," News Release No. 20080802, http://www.hqusareur.army.mil/news/releases/2008-08-27-02_transformation.pdf (accessed 12 September 2008).
26. 5th Signal Command, "5th Signal Command Booklet," 11, <http://www.5sigcmd.army.mil/publications/5thSigBooklet.pdf>, (accessed 12 September 2008).
27. Ibid.
28. MaryAnn Lawlor, "Intelligence Cell Defends Cyberspace," *SIGNAL Magazine*, August 2008, http://www.afcea.org/signal/articles/templates/Signal_Article_Template.asp?articleid=1663&zoneid=238 (accessed 5 September 2008).
29. Ibid.

30. 5th Signal Command, "5th Signal Command Booklet," 11, <http://www.5sigcmd.army.mil/publications/5thSigBooklet.pdf>, (accessed 12 September 2008).
31. Ibid. 11.
32. Ibid. 11.
33. MaryAnn Lawlor, "Intelligence Cell Defends Cyberspace," *SIGNAL Magazine*, August 2008, http://www.afcea.org/signal/articles/templates/Signal_Article_Template.asp?articleid=1663&zoneid=238 (accessed 5 September 2008).
34. Kristopher Joseph, "Team Works to Defend Digital Battlefield in Europe," *American Forces Press Service*, 31 December 2007, <http://www.defenselink.mil/news/newsarticle.aspx?id=48544> (accessed 15 September 2008).
35. MaryAnn Lawlor, "Intelligence Cell Defends Cyberspace," *SIGNAL Magazine*, August 2008, http://www.afcea.org/signal/articles/templates/Signal_Article_Template.asp?articleid=1663&zoneid=238 (accessed 5 September 2008).
36. U.S. Army, *Signal Support to Theater Operations*, Field Manual Interim (FMI) 6-02.45 (Washington, DC: Headquarters Department of the Army, 5 July 2007), <http://www.fas.org/irp/doddir/army/fmi6-02-45.pdf> (accessed 26 September 2008), 3-10.
37. Ibid., 3-10.
38. 5th Signal Command, "5th Signal Command Booklet," 11, <http://www.5sigcmd.army.mil/publications/5thSigBooklet.pdf>, (accessed 12 September 2008).
39. Chairman, U.S. Joint Chiefs of Staff, *DOD Dictionary of Military and Associated Terms*. Joint Publication (JP) 1-2 (Washington, DC: CJCS, 12 April 2001 as amended through 26 August 2008), http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf (accessed September and October 2008), 273-274.
40. Charles E. Croom, Jr., "Cyberspace: Global Network Operations," *Joint Forces Quarterly*, no. 46 (3rd Quarter 2007), 70.

Appendix A: Joint Task Force – Global Network Operations Responsibilities

JTF-GNO Responsibilities taken directly from USSTRATCOM's *Joint Concept of Operations for Global Information Grid NetOps, Version 3*, pages 16-17:

- Direct GIG NetOps to ensure confidentiality, integrity, availability and efficiency of the GIG infrastructure and information services.
- Establish and maintain situational awareness of the GIG and report readiness and defensive posture to HQ USSTRATCOM, as required.
- Coordinate with HQ USSTRATCOM staff and subordinate organizations, as required.
- Assist in identifying, establishing and maintaining GIG NetOps characteristics, capabilities, standards and requisite measures of effectiveness for infrastructure and information services.
- Direct and oversee network operations and defense capabilities.
- Ensure that computer network operations are synchronized for crisis and deliberate planning.
- Develop course of action recommendations for NetOps, including CND and CND response actions, in support of USSTRATCOM and national strategic objectives.
- Establish procedures to conduct CND response actions in accordance with DOD policy and coordinate with JFCC-NW for Tier 1 computer network defense response actions.
- Oversee procedures to establish and provide measures of effectiveness and damage assessments.
- Provide support for USSTRATCOM and other geographic and functional Combatant Commanders' exercises, wargames and experimentation requirements involving NetOps.
- Provide network defense priority intelligence requirements, requests for intelligence, intelligence production requirements and intelligence collection requirements with USSTRATCOM J2 for tasking, deconfliction and accomplishment.
- Perform all-source analysis of threats to the GIG.
- Establish a relationship with mission area experts in the regional commander's Standing Joint Force Headquarters to provide operational support for NetOps with emphasis on CND.

- Support USSTRATCOM development and execution of NetOps assessments, research and development efforts and advocacy of capability needs.
- Support USSTRATCOM and Joint Force Component Commands' led efforts to create and maintain strategic-level OPLANs.
- Develop and coordinate NetOps Concept of Operations.

Appendix B: Theater Network Operations Center (TNC) Responsibilities

Theater NetOps Center Responsibilities taken directly from USSTRATCOM's *Joint Concept of Operations for Global Information Grid NetOps, Version 3*, pages 22-23:

- Operate and maintain the backbone services of the GIG assets located in its theater.
- Collaborate with the NetOps community to ensure effective operation and defense of the GIG.
- Issue technical directives to Network Operations Security Centers.
- Receive situational awareness information in order to monitor all Theater, Service and/or Service Component, and Agency systems and networks designated as mission critical.
- Support Theater, Service and/or Service Components, and Agencies by creating, disseminating, and making available the NetOps SA views for them.
- Coordinate with the TNCC regarding reporting requirements.
- Monitor and collect performance data continuously for those information resources deemed important by the TNCC.
- Provide system and network status information as part of the situational awareness view.
- Provide the TNCC or the Global NetOps Coordination Center with information security products and services.
- Assist in determining the technical and operational mission impacts caused by degradations, outages, and global network defense (GND) events.
- Perform incident/intrusion monitoring and detection, strategic vulnerability analysis, media analysis, and responses to GND-related activity.
- Determine courses of action and direct restoral of capabilities and services when required.
- Maintain situational awareness for each GCC's current and near term operations and plans.
- Maintain security monitoring through an integrated GIG situational awareness theater view.
- Identify and resolve computer security anomalies that affect GIG assets located in their theater.
- Coordinate theater GND support as directed by the TNCC.

- Coordinate with and receive support from the Law Enforcement/Counterintelligence community.
- Manage Joint Spectrum Interference Resolution (JSIR) access for the theater.
- Manage apportioned satellite communication resources.

Appendix C: Theater Network Operations Control Center (TNCC) Responsibilities

Theater NetOps Control Center Responsibilities taken directly from USSTRATCOM's *Joint Concept of Operations for Global Information Grid NetOps, Version 3*, pages 26-27:

- Establish uniform round-the-clock visibility into the status of the GIG situational awareness view from/to TNC and assigned NetOps organizations.
- Collaborate with the NetOps Community to ensure effective operation and defense of the GIG.
- Establish and retain visibility of system and network outages and customer service shortfalls.
- Direct reporting of NetOps events, conduct analysis of the impact of such events on the operational mission, develop alternate courses of action, and advise the CDR and other senior decision makers on the status of GIG degradations, outages, GND events, and areas requiring improvement.
- Prioritize the installation and restoration of system and network services for the TNC and subordinate organizations in the form of a critical customer listing.
- Direct, coordinate, and integrate response actions to computer network attacks and significant intrusions affecting the GCC's portion of the GIG.
- Direct the theater's response to JTF-GNO directives for correcting or mitigating global NetOps issues.
- Coordinate with JTF-GNO to de-conflict the GCC Theater NetOps priorities with the global NetOps priorities of JTF-GNO and USSTRATCOM.
- Deconflict issues between the TNC and the Network Operations Security Centers.

Abbreviations

CCDR	Combatant Commander
CND	Computer Network Defense
CNO	Computer Network Operations
CTIC	Cyber-Threat Intelligence Cell
DISA	Defense Information Systems Agency
DOD	Department of Defense
FMI	U.S. Army Field Manual Interim
GCC	Geographic Combatant Command
GIG	Global Information Grid
ISR	Intelligence, Surveillance and Reconnaissance
ISR	Internet Surveillance and Reconnaissance
JP	Joint Publication
JTF-GNO	Joint Task Force for Global Network Operations
NetOps	Network Operations
NMS-CO	National Military Strategy for Cyberspace Operations
NMS-CO I-plan	National Military Strategy for Cyberspace Operations Implementation Plan
OPCON	Operational Control
TACON	Tactical Control
TNC	Theater Network Operations Center
TNCC	Theater Network Operations Control Center
USAREUR	U.S. Army European Theater
USEUCOM	United States European Command
USSTRATCOM	United States Strategic Command

Glossary

All entries in this glossary are quoted directly from JP 1-2, *DOD Dictionary of Military and Associated Terms*, 12 April 2001 as amended through 26 August 2008.

combatant command (command authority) — Nontransferable command authority established by title 10 (“Armed Forces”), United States Code, section 164, exercised only by commanders of unified or specified combatant commands unless otherwise directed by the President or the Secretary of Defense. Combatant command (command authority) cannot be delegated and is the authority of a combatant commander to perform those functions of command over assigned forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction over all aspects of military operations, joint training, and logistics necessary to accomplish the missions assigned to the command. Combatant command (command authority) should be exercised through the commanders of subordinate organizations. Normally this authority is exercised through subordinate joint force commanders and Service and/or functional component commanders. Combatant command (command authority) provides full authority to organize and employ commands and forces as the combatant commander considers necessary to accomplish assigned missions. Operational control is inherent in combatant command (command authority). Also called **COCOM**.

computer network attack — Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. Also called **CNA**.

computer network defense — Actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within the Department of Defense information systems and computer networks. Also called **CND**.

computer network exploitation — Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks. Also called **CNE**.

computer network operations — Comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations. Also called **CNO**.

Global Information Grid - The globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The Global Information Grid includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services and National Security Systems. Also called **GIG**.

network operations — Activities conducted to operate and defend the Global Information

Grid. Also called **NETOPS**.

operational control - Command authority that may be exercised by commanders at any echelon at or below the level of combatant command. Operational control is inherent in combatant command (command authority) and may be delegated within the command. Operational control is the authority to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission. Operational control includes authoritative direction over all aspects of military operations and joint training necessary to accomplish missions assigned to the command. Operational control should be exercised through the commanders of subordinate organizations. Normally this authority is exercised through subordinate joint force commanders and Service and/or functional component commanders. Operational control normally provides full authority to organize commands and forces and to employ those forces as the commander in operational control considers necessary to accomplish assigned missions; it does not, in and of itself, include authoritative direction for logistics or matters of administration, discipline, internal organization, or unit training. Also called **OPCON**.

tactical control - Command authority over assigned or attached forces or commands, or military capability or forces made available for tasking, that is limited to the detailed direction and control of movements or maneuvers within the operational area necessary to accomplish missions or tasks assigned. Tactical control is inherent in operational control. Tactical control may be delegated to, and exercised at any level at or below the level of combatant command. Tactical control provides sufficient authority for controlling and directing the application of force or tactical use of combat support assets within the assigned mission or task. Also called **TACON**.

Bibliography

- 5th Signal Command official Web site. <http://www.5sigcmd.army.mil/> (accessed 5, 12 September 2008).
- 5th Signal Command. "5th Signal Command Booklet." *5th Signal Command official Web site*. <http://www.5sigcmd.army.mil/publications/5thSigBooklet.pdf> (accessed 12 September 2008, subsequently replaced by <http://www.5sigcmd.army.mil/publications/5thSigBooklet2008web.pdf>).
- "Air Intelligence Agency renamed for new Internet Role." *Air Force Link*, 15 May 2007. <http://www.humorcontrol.org/usaf/pr/> (accessed 5 September 2008).
- Alberts, David S., John J. Garstka, Richard E. Hayes, and David T. Signori. *Understanding Information Age Warfare*. Washington, DC: DOD Command and Control Research Program, 2004.
- Alexander, Keith B. "Warfighting in Cyberspace." *Joint Forces Quarterly*, no. 46 (3rd Quarter 2007): 58-61.
- Armistead, Leigh. *Information Operations: Warfare and the Hard Reality of Soft Power*. Washington, DC: Brassey's Inc., 2004.
- Army Study Guide Web Site. "5th Signal Command." *Army Study Guide*, 14 July 2006. <http://www.armystudyguide.com> (accessed 12 September 2008).
- Baker, Fred W. "Recent Cyber Attacks Serve as Lesson, General Says." *American Forces Press Service*, 24 August 2008. <http://www.defenselink.mil/news/newsarticle.aspx?id=50910> (accessed 15 September 2008).
- Buxbaum, Peter A. "Battling Botnets." *Military Information Technology* 12, no. 7 (20 August 2008). <http://www.mit-kmi.com/article.cfm?DocID=2569> (accessed 26 September 2008).
- Castelli, Christopher J. "Defense Department Adopts New Definition for Cyberspace." *Inside the Air Force*, 23 May 2008. <http://integrator.hanscom.af.mil/2008/May/05292008/05292008-24.htm> (accessed 15 September 2008).
- Coleman, Kevin G. "Department of Cyber Defense: An Organization Who's Time Has Come." *Technolytics*, November 2007. http://www.technolytics.com/Dept_of_Cyber_Defense.pdf (accessed 15 September 2008).

- Croom, Charles E., Jr. "Cyberspace: Global Network Operations." *Joint Forces Quarterly*, no. 46 (3rd Quarter 2007): 69-70.
- Elliott, Michael C. "Operational Command and Control of Joint Task Force Cyberspace Operations." Research Paper, Newport, RI: U.S. Naval War College, Joint Military Operations Department, 2008.
- Fraley, Michelle M. "The BORG: Network Centric Operations." Research Paper, Newport, RI: U.S. Naval War College, Joint Military Operations Department, 2006.
- Halpin, Edward, Philippa Trevorrow, David Webb, and Steve Wright, ed. *Cyberwar, Netwar and the Revolution in Military Affairs*. Hampshire England: Palgrave MacMillan, 2006.
- Hunt, Carl and Nancy Chesser, ed. *Deterrence 2.0: Detering Violent Non-State Actors in Cyberspace*. Workshop Proceedings, Arlington, VA: U.S. Strategic Command Global Innovation and Strategy Center, January 2008.
http://www.insidedefense.com/secure/data_extra/pdf7/dplus2008_2657.pdf (accessed 13 October 2008).
- Joseph, Kristopher. "Team Works to Defend Digital Battlefield in Europe." *American Forces Press Service*, 31 December 2007.
<http://www.defenselink.mil/news/newsarticle.aspx?id=48544> (accessed 15 September 2008).
- Kenyon, Henry S. "Training Vital to Network Defense." *SIGNAL Magazine*, August 2008.
http://www.afcea.org/signal/articles/templates/Signal_Article_Template.asp?articleid=1665&zoneid=238 (accessed 5 September 2008).
- Lawlor, MaryAnn. "Intelligence Cell Defends Cyberspace." *SIGNAL Magazine*, August 2008.
http://www.afcea.org/signal/articles/templates/Signal_Article_Template.asp?articleid=1663&zoneid=238 (accessed 5 September 2008).
- Lenfant, Babette M. "Protecting Our Critical Information Technology Systems." Research Paper, Newport, RI: U.S. Naval War College, Joint Military Operations Department, 2003.
- Lentz, Robert. "Cyber-Security Focus Today is on Securing the Networks That Our Warfighters Depend on to Perform Their Missions." *Military Information Technology* 12, no. 6 (3 July 2008). <http://www.mit-kmi.com/article.cfm?DocID=2538> (accessed 15 September 2008).
- Lord, William T. "Preparing Combat Forces for the Electromagnetic Spectrum." Interview by Harrison Donnelly, *Military Information Technology* 12, no. 3 (9 April 2008).
<http://www.mit-kmi.com/article.cfm?DocID=2395> (accessed 26 September 2008).

- Raduege, Harry D, Jr. "Future Defense Department Cybersecurity Builds on the Past." *SIGNAL Magazine*, February 2008.
http://www.afcea.org/signal/articles/templates/Signal_Article_Template.asp?articleid=1493&zoneid=226 (accessed 26 September 2008).
- Ranne, Wayne K., Larry K. McKee, Jr. *Global Information Grid NetOps Tasking Orders (GNTO)*. White paper. Smithfield, VA: Select Innovation, 28 June 2006.
<http://www.selectinnovation.com/Published%20Articles/2006-06-28-GIG%20Network%20Tasking%20Order.pdf> (accessed 15 September 2008).
- Schneider, Kent R. "Information Assurance is the Ultimate Joint Endeavor." *SIGNAL Magazine*, August 2008.
http://www.afcea.org/signal/articles/templates/Signal_Article_Template.asp?articleid=1671&zoneid=238 (accessed 5 September 2008).
- Stump, Adam M. "Vice Chairman Cites Need for Cyber Warfare Experimentation." *American Forces Press Service*, 20 June 2008.
<http://www.defenselink.mil/news/newsarticle.aspx?id=50273> (accessed 15 September 2008).
- U.S. Army. *Signal Support to Theater Operations*. Field Manual Interim (FMI) 6-02.45. Washington, DC: Headquarters Department of the Army, 5 July 2007.
<http://www.fas.org/irp/doddir/army/fmi6-02-45.pdf> (accessed 26 September 2008).
- U.S. Army Europe & 7TH Army Office of the Chief of Public Affairs. "USAREUR Announces FY09 Transformation Actions." News Release No. 20080802.
http://www.hqusareur.army.mil/news/releases/2008-08-27-02_transformation.pdf (accessed 12 September 2008).
- U.S. Department of Defense. *Computer Network Defense*. Department of Defense Directive (DODD) O-8530.1. Washington, DC: DOD, 8 January 2001.
https://powhatan.iie.disa.mil/cnd/DODD_O_8530-1.pdf (accessed 15 September 2008). (Unclassified//For Official Use Only) Information extracted is unclassified.
- U.S. Department of Defense. *National Defense Strategy*. Washington, DC: DOD, June 2008.
- U.S. Office of the Chairman of the Joint Chiefs of Staff. *DOD Dictionary of Military and Associated Terms*. Joint Publication (JP) 1-2. Washington, DC: CJCS, 12 April 2001 as amended through 26 August 2008. http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf (accessed multiple dates in September and October 2008).
- U.S. Office of the Chairman of the Joint Chiefs of Staff. *Information Operations*. Joint Publication (JP) 3-13. Washington, DC: CJCS, 13 February 2006.

- U.S. Office of the Chairman of the Joint Chiefs of Staff. *Joint Communications Systems*. Joint Publication (JP) 6.0. Washington, DC: CJCS, 20 March 2006.
- U.S. Office of the Chairman of the Joint Chiefs of Staff. *Information Assurance (IA) and Computer Network Defense (CND)*. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.01E. Washington, DC: CJCS, 15 August 2007, current as of 12 August 2008. http://www.dtic.mil/cjcs_directives/cdata/unlimit/6510_01.pdf (accessed 15 September 2008).
- U.S. Office of the Chairman of the Joint Chiefs of Staff. *The National Military Strategy of the United States of America: A Strategy for Today; A Vision for Tomorrow*. Washington, DC: CJCS, 2004.
- U.S. Office of the Chairman of the Joint Chiefs of Staff. *The National Military Strategy for Cyberspace Operations* (U). Washington, DC: CJCS, 2006.
<http://www.dod.mil/pubs/foi/ojcs/07-F-2105doc1.pdf> (accessed 12 September 2008).
(Unclassified version of Secret document).
- U.S. Office of the Chairman of the Joint Chiefs of Staff, *The National Military Strategy for Cyberspace Operations Implementation Plan* (U). Washington, DC: CJCS, 24 September 2007.
http://scie.stratcom.smil.mil/sites/restrictedWorkspaces/8039_ICP/StrategyGuidance/NMS-CO-NationalMilitaryStrategyforCyberspaceOperations2007.doc/ (accessed 12 September 2008). (Secret) Information Extracted is unclassified.
- U.S. President. *The National Strategy to Secure Cyberspace, February 2003*. Washington, DC: White House, 2003.
- U.S. President. *The National Security Strategy of the United States of America, September 2002*. Washington, DC: White House, 2002.
- U. S. Strategic Command. *Joint Concept of Operations for Global Information Grid NetOps, Version 3* (U), 4 August 2006.
http://jtfigno.smil.mil/site/Documents/NetOpsCONOPS/GIG_NetOps_CONOPS_Verson3_4_Aug_06.pdf/ (accessed 12 September 2008). (Unclassified//For Official Use Only)
Information extracted is unclassified.
- U.S. Strategic Command. *Joint Task Force - Global Network Operations Fact Sheet*, November 2007. http://www.stratcom.mil/fact_sheets/fact_jtf_igno.html (accessed 26 September 2008).
- Virdon, Roy John. "Critical Vulnerability: Defending the Decisive Point of United States Computer Networked Information Systems." Research Paper, Newport, RI: U.S. Naval War College, Joint Military Operations Department, 2003.